1 RW AF

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	10/000,154
Filing Date	October 23, 2001
First Named Inventor	Koteshwerrao S. Adusumilli
Art Unit	2134
Examiner Name	Christopher Brown
Total Number of Pages in This Submission	29
Attorney Docket Number	42390P12318

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
  - ☐ PTO/SB/08
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Basic Filing Fee
  - ☐ Declaration/POA
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below):*

Return postcard

Remarks

Per MPEP 1204.01, any previously paid appeal fees set forth in 37 CFR 41.20 for filing an Appeal Brief will be applied to the new Appeal Brief in the same application as long as a final Board decision has not been made on the prior appear.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Brent E. Vecchia, Reg. No. 48,011 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	Brent E. Vecchia
Date	May 5, 2008

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	**Debbie Casias**		
Signature	Debbie Casias	Date	**May 5, 2008**

FEE TRANSMITTAL for FY 2007

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT	($)

Complete if Known	
Application Number	10/000,154
Filing Date	October 23, 2001
First Named Inventor	Koteshwerrao S. Adusumilli
Examiner Name	Christopher Brown
Art Unit	2134
Attorney Docket No.	42390P12318

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ None ☒ Other (please identify): Charge Deposit Account

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20. ☒ Credit any overpayments

FEE CALCULATION

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	460	2252	230	Extension for reply within second month	
1253	1,050	2253	525	Extension for reply within third month	
1254	1,640	2254	820	Extension for reply within fourth month	
1255	2,230	2255	1,115	Extension for reply within fifth month	
1401	510	2401	255	Notice of Appeal	
1402	510	2402	255	Filing a brief in support of an appeal	
1403	1,030	2403	515	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	810	1809	405	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	810	2810	405	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) _____

SUBTOTAL (2) ($)

SUBMITTED BY Complete (if applicable)

Name (Print/Type)	Brent E. Vecchia	Registration No. (Attorney/Agent)	48,011	Telephone	(303) 740-1980
Signature	Brent E. Vecchia			Date	05/05/08

Based on PTO/SB/17 (12-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 12/15/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Patent Application of:	)	
	)	
Adusumilli et al.	)	
	)	
Serial No.: 10/000,154	)	Art Unit: 2134
	)	
Filed: 10/23/2001	)	
	)	Examiner: Christopher J. Brown
For: SELECTING A SECURITY FORMAT CONVERSION FOR WIRED AND WIRELESS DEVICES	)	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF (SECOND)
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

This brief is in furtherance of the Notice of Appeal, filed in the above-captioned case on 3/3/08. This second appeal brief is filed after prosecution was reopened by the mailing of the Office Action on 12/12/07 after submission of a first appeal brief on 8/21/07. Applicants (hereafter "Appellants") hereby submit this Brief (37 C.F.R. § 41.37). The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying Transmittal of Appeal Brief. Appellants respectfully request consideration of this appeal by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37c(1)):

Page 17 of this brief bears the practitioner's signature.

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California, 95052, to whom the invention is assigned.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

With respect to other appeals or interferences that will directly affect, or be affected by, or have a bearing on the Board's decision in this appeal, to the best of Appellant's knowledge, there are no such appeals or interferences.

III. STATUS OF THE CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

The status of the claims in this application are:

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims 18-48 are currently pending in the application.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: 1-17
2. Claims withdrawn from consideration but not cancelled: NONE
3. Claims pending: 18-48
4. Claims allowed: NONE
5. Claims rejected: 18-48

C. CLAIMS ON APPEAL

Claims 18-48 are on appeal.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

A response was submitted in response to the Final Office Action mailed on February 21, 2007. The response included amendments to the claims. At the time of filing the initial Appeal Brief on 8/21/2007, the Examiner had not entered these amendments. The Examiner later re-opened prosecution with the mailing of an Office Action on 12/12/07. In the Office Action, the Examiner referred to the Appeal Brief dated 8/21/07 and did not indicate that the amendments to the claims in the response to the Final Office Action mailed on February 21, 2007 were entered. Appellants phoned the Examiner on 5/1/08 and 5/5/08 and phoned the Examiner's supervisor on 5/5/08 to inquire whether the amendments have been entered. However, Appellants were unable to reach the Examiner or the Examiner's supervisor. Since the last Office Action refers to the Appeal Brief and does not indicate that the amendments were entered, Appellants assume that these amendments have not been entered. A copy of all claims on appeal is attached hereto as an appendix of claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

Embodiments of the invention pertain to selecting a security format conversion for wired and wireless devices. See e.g., the Title.

Independent claim 18 pertains to a system according to a first embodiment of the invention. See e.g., paragraph [0024]; security system 645 in Figure 6; paragraph [0046]; selection system 1100 in Figure 11; security system 1220 in Figure 12; and security system 1300 in Figure 13. The system includes a network interface. See e.g., network interface 650 in Figure 6; paragraph [0047]; and network link 1321 in Figure 13. The network interface is couplable with a public network (e.g., public network 625 in Figure 6) to receive a first client message and first data that is encrypted according to a wireless security format. See e.g., paragraph [0047]; WTLS data in Figure 6; block 730 in Figure 7; and component 960 in Figure 9. The network interface is also to receive a second client message and second data that is encrypted according to a wired security format. See e.g., paragraph [0047]; SSL data in Figure 6; and block 755 in Figure 7. The system also includes a selection system coupled with the network interface. See e.g., selection system 660 in Figure 6; paragraph [0048]; and selection system 1100 in Figure 11. The selection system is to select a first security format conversion for the first data and to select a second security format conversion for the second data. See e.g., paragraph [0048]; and blocks 725 and 750 in Figure 7. The system also includes a conversion system coupled with the selection system. See e.g., conversion system 670 in Figure 6; and paragraphs [0053]-[0054]. The conversion system is to perform the first security format conversion on the first wireless security format encrypted data and to perform the second security format conversion on the second wired security format encrypted data. See e.g., paragraphs [0053]-[0054]; blocks 735 and 760 in Figure 7; and WTLS conversion system 672 and SSL conversion system 674 in Figure 6.

Independent claim 29 pertains to a method according to a second embodiment of the invention. See e.g., method 700 of Figure 7; and paragraphs [060] through [0075]. The method includes listening on a network interface for a first client message and first data that is encrypted according to a security format for wireless data. See e.g., listening at block 710 of Figure 7; and paragraph [0063]. The method also includes listening on the network interface for a second client message and second data that is encrypted according to a security format for wired data. See e.g., listening at block 710 of Figure 7; and paragraph [0063]. The method also includes receiving the first client message and the second client message from the network interface. See e.g., WTLS data and SSL data in Figure 6; blocks 730 and 755 in Figure 7; and paragraphs [0068] and [0072]. The method also includes selecting a first security format conversion for the first data and selecting a second security format conversion for the second data. See e.g., selection system 660 in Figure 6; blocks 725 and 750 in Figure 7; and paragraphs [0066] and [0071]. The method also includes performing the first security format conversion on the first data and performing the second security format conversion on the second data. See e.g., conversion system 670 in Figure 6; and blocks 735 and 760 in Figure 7; and paragraphs [0068] and [0072].

Independent claim 36 pertains to a machine-readable medium according to a third embodiment of the invention. See e.g. original claim 15. The machine-readable medium has stored thereon data representing sequences of instructions that if executed cause a machine to perform operations. See e.g. original claim 15; and paragraphs [060] through [0075]. The operations include listening on a network interface for a first client message and first data that is encrypted according to a security format for wireless data. See e.g., listening at block 710 of Figure 7; and paragraph [0063]. The operations also include listening on the network interface for a second client message and second data that is encrypted according to a security format for wired data. See e.g., listening at block 710

of Figure 7; and paragraph [0063]. The operations also include receiving the first client message and the second client message from the network interface. See e.g., WTLS data and SSL data in Figure 6; blocks 730 and 755 in Figure 7; and paragraphs [0068] and [0072]. The operations also include selecting a first security format conversion for the first data and selecting a second security format conversion for the second data. See e.g., selection system 660 in Figure 6; blocks 725 and 750 in Figure 7; and paragraphs [0066] and [0071].

Independent claim 40 pertains to a method according to a fourth embodiment of the invention. See e.g., method 700 of Figure 7. The method includes receiving an indication of one of a plurality of ports on which a client message was received from a public network. See e.g., indication 430B in Figure 4; the WTLS data received at port 654 and the SSL data received at port 652 in Figure 6; and blocks 715 and 740 in Figure 7. The method also includes selecting a security format conversion from among a plurality of format conversions. See e.g., selection system 470 in Figure 4; selection system 660 in Figure 6; and blocks 725 and 750 of Figure 7. The plurality include a first security format conversion from a Wireless Transport Layer Security format to another format. See e.g., WTLS conversion system 672 in Figure 6; and block 725 in Figure 7. The plurality also include a second security format conversion from a Secure Sockets Layer security format to another format See e.g., SSL conversion system 674 in Figure 6; and block 750 in Figure 7. This may be performed in dependence upon the received indication of the port. See e.g., indication 430B in Figure 4; and paragraph [0029].

Independent claim 47 pertains to a system according to a fifth embodiment of the invention. See e.g., paragraph [0024]; security system 645 in Figure 6; paragraph [0046]; selection system 1100 in Figure 11; security system 1220 in Figure 12; and security system 1300 in Figure 13. The system includes a first network interface within a data center and couplable with a public network. See e.g., network interface 650 in Figure 6;

paragraph [0047]; and network link 1321 in Figure 13. Figure 6 shows that the security system 645 is within data center 640. Figure 4 also shows security system 460 within data center 450. The interface is to receive a first Wireless Transport Layer Security encrypted data from a cell phone client. See e.g., paragraph [0047]; WTLS data in Figure 6; and block 730 in Figure 7. Wireless access device 605, which may be a cell phone client, is shown in Figure 6. The interface is also to receive a second Secure Sockets Layer encrypted data from a personal computer client. See e.g., paragraph [0047]; SSL data in Figure 6; and block 755 in Figure 7. Wired access device 620, which may be a personal computer client, is shown in Figure 6. The system also includes a conversion system within the data center. See e.g., conversion system 670 in Figure 6; and paragraphs [0053]-[0054]. The conversion system is to convert the first Wireless Transport Layer Security encrypted data received from the cell phone client to plain data. See e.g., WTLS conversion system 672 to convert the WTLS data to plain data in Figure 6; block 735 in Figure 7; and paragraphs [0053]-[0054]. The conversion system is also to convert the second Secure Sockets Layer encrypted data received from the personal computer client to plain data. See e.g., SSL conversion system 674 to convert the SSL data to plain data in Figure 6; block 760 in Figure 7; and paragraphs [0053]-[0054]. The system also includes a second network interface within the data center that is couplable with a private network to provide the plain data to the private network. See e.g., paragraph [0046]; network interface 680 in Figure 6; paragraph [0055]; and server link 1322 in Figure 13. See e.g., server 690 in data center 640.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

A. Claims 18-48 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. US2002/0133598 by Strahm.

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

A. REJECTION OF CLAIMS 18-48 UNDER 35 U.S.C. § 102(E) AS BEING ANTICIPATED BY U.S. PATENT APPLICATION PUBLICATION NO. US2002/0133598 BY STRAHM IS IMPROPER.

GROUP I: CLAIMS 18-46

The Examiner has rejected claims 18-48 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. US2002/0133598 by Strahm (hereinafter referred to as "Strahm"). Appellants respectfully submit that the present claims are not anticipated by Strahm.

Claim 18 recites a system comprising:

"a network interface couplable with a public network to receive ***a first client message and first data that is encrypted according to a wireless security format*** *and to receive* ***a second client message and second data that is encrypted according to a wired security format;***

a selection system coupled with the network interface to select a first security format conversion for the first data and to select a second security format conversion for the second data; and

a conversion system coupled with the selection system to perform the first security format conversion on the first wireless security format encrypted data and to perform the second security format conversion on the second wired security format encrypted data".

Strahm does not disclose these limitations. In particular, Strahm does not disclose a system including a network interface couplable with a public network to receive **a first client message and first data that is encrypted according to a wireless security format** and **a second client message and second data that is encrypted according to a wired security format.** Nor does Strahm disclose the claimed selection system, or the claimed conversion system to perform the first selected security format conversion on the first **wireless security format**

encrypted data and to perform the second selected security format conversion on the second **wired security format encrypted data.**

Strahm pertains to network communication. See e.g., the Title. Strahm discusses that the mobile device 110 of FIG. 1 may communicate with a home agent 160 of Figure 1. The mobile device 110 may establish four exemplary connections or tunnels with the home agent 160. See e.g., paragraph [0011]. Connection 114 is a wireless phone link, connection 116 is a wireless connection, connection 118 is a wired network connection, and connection 120 is a direct connection to the Internet 140. See e.g., paragraphs [0013] through [0016]. More than one connection may be active at a given time. See e.g., paragraph [0022]. Either the same or different security protocols may be used for the different connections. See e.g., paragraphs [0025] and [0026].

As explained in paragraph [0024], security protocols are established and authenticated. Paragraph [0024] mentions that examples of security protocols include transport layer security (TLS), secure sockets layers (SSL), and wireless TLS (WTLS). As understood by Appellants, this is the only mention of WTLS in the entire application.

However, Applicants respectfully submit that paragraph [0024] discloses that WTLS is an example of a security protocol for the **mobile client** 110 (emphasis added). There is no disclosure that the home agent 160 use WTLS, or any other wireless security format. There is absolutely no disclosure that the home agent 160 receives first data that is encrypted according to WTLS and a second data that is encrypted according to SSL. In fact, 766/776 in FIG. 7 seem to suggest that only TLS/SSL is used.

With reference to FIG. 1 of Strahm, notice that the wireless phone link connection 114 and the wireless connection 116 each go through one or more components (e.g., a tower and the Internet, etc.). At some point these connections become wired instead of wireless. Strahm is silent on the security processing that may occur, since presumably it does not pertain to the invention.

However, as understood by Appellants, WTLS encrypted data would typically be converted to another format, such as SSL, within a WAP gateway (see e.g., Figures 1-2 of the present patent application), or within a trusted WTLS/SSL conversion system (see e.g., Figure 3 of the present patent application), or otherwise, prior to reaching the home agent 160. Such format conversion would result in the home agent receiving SSL or other wired encrypted data, but not WTLS encrypted data, or any other type of wirelessly encrypted data. This seems consistent with the TLS/SSL indicated at 766/776 in FIG. 7 of Strahm.

In any event, Strahm does not specifically disclose that the home agent 160 receives WTLS data, or any other data encrypted according to a wirelessly security format. Furthermore, the Examiner has not provided sufficient reasoning as to how WTLS data may remain encrypted throughout its traversal from the mobile device 110 through the Internet to the home agent 160. Furthermore, the anticipation standard requires that every element be identically shown.

Furthermore, the mobile client 110 of Strahm is on the **client** side. As understood by Applicants, the mobile client 110 does not receive the claimed **client** messages.

Appellants also point out that anticipation under 35 U.S.C. Section 102 requires every element of the claimed invention be identically shown in a single prior art reference. The Federal Circuit has indicated that the standard for measuring lack of novelty by anticipation is strict identity. "*For a prior art reference to anticipate in terms of 35 U.S.C. Section 102, every element of the claimed invention must be identically shown in a single reference.*" In Re Bond, 910 F.2d 831, 15 USPQ.2d 1566 (Fed. Cir. 1990).

Accordingly, Appellants respectfully submit that claim 18 is not anticipated by Strahm. The dependent claims of claim 18 are believed to be allowable therefor, as well as for the recitations set forth in each of these dependent claims. Independent claims 29, 36, and 40, and their respective dependent claims, are believed to be allowable for similar reasons.

For at least these reasons, the claims of Group I (claims 18-46) are believed to be allowable over Strahm.

GROUP II: CLAIMS 47-48

Claim 47 recites a system comprising:

"a first network interface within a data center and couplable with a public network to receive a first Wireless Transport Layer Security encrypted data from a cell phone client and to receive a second Secure Sockets Layer encrypted data from a personal computer client;

a conversion system within the data center to convert the first Wireless Transport Layer Security encrypted data received from the cell phone client to plain data and to convert the second Secure Sockets Layer encrypted data received from the personal computer client to plain data;

a second network interface within the data center and couplable with a private network to provide the plain data to the private network".

Strahm does not disclose these limitations. In particular, Strahm does not disclose the claimed first interface that is **within a data center** and that receives the first **Wireless Transport Layer Security encrypted data** from a **cell phone client** and that receives the second **Secure Sockets Layer encrypted data** from a **personal computer client**. As discussed above, there is no disclosure that the home agent 160 receive Wireless Transport Layer Security encrypted data. The recitation of "within a data center", "from a cell phone client", "from a personal computer client", and "a second network interface within the data center" further help to rule out the mobile device 110. Nor does Strahm disclose the claimed conversion system.

Accordingly, Appellants respectfully submit that claim 47 is not anticipated by Strahm. Claim 48 depends on claim 47 and is believed to be allowable therefor, as well as for the recitations set forth therein.

For at least these reasons, the claims of Group II (claims 47-48) are believed to be allowable over Strahm.

GROUP III: CLAIMS 43-46

Claim 43 is a dependent claim from claim 18 that recites "*further comprising a second network interface to provide the plain data*". There is no disclosure in Strahm that the mobile device 110 has this claimed second network interface to provide the plain data. Accordingly, claim 43 is believed to be further allowable over Strahm. Dependent claims 44-46 are believed to be further allowable over Strahm for one or more similar reasons. For at least these reasons, the claims of Group III (claims 43-46) are believed to be further allowable over Strahm.

GROUP IV: CLAIMS 28, 34, and 38

Claim 28 is a dependent claim from claim 18 that recites "*residing in a data center between a first switch within the data center and a second switch within the data center*". There is no disclosure in Strahm that the home agent 160 or the mobile device 110 of Strahm meets these limitations of "*residing in a data center between a first switch within the data center and a second switch within the data center*". Accordingly, claim 28 is believed to be further allowable over Strahm. Dependent claims 34 and 48 are believed to be further allowable over Strahm for one or more similar reasons. For at least these reasons, the claims of Group IV (claims 28, 34, and 38) are believed to be further allowable over Strahm.

GROUP V: CLAIMS 27 and 33

Claim 27 is a dependent claim from claim 18 that recites "*residing in a data center between the Internet and a data center server*". There is no disclosure in Strahm that the mobile device 110 of Strahm resides in a data center between the Internet and a data center server. Accordingly, claim 27 is believed to be further allowable over Strahm. Dependent claim 33 is believed to be further allowable over Strahm for one or more similar reasons. For at least these reasons, the claims of Group V (claims 27 and 33) are believed to be further allowable over Strahm.

GROUP VI: CLAIMS 20, 21, 30, 37, 41

Claim 20 is a dependent claim from claim 18 that recites "*wherein the first port has a number selected from the group consisting of the numbers 9208 through 9282, and wherein the second port has number 443*". Strahm does not disclose this limitation and the Examiner has not provided sufficient reason why it would be inherent. Furthermore,

this limitation further distinguishes over the Mobile device 110. Accordingly, claim 20 is believed to be further allowable over Strahm. Dependent claims 21, 30, 37, 41 are believed to be further allowable over Strahm for one or more similar reasons. For at least these reasons, the claims of Group VI (claims 20, 21, 30, 37, 41) are believed to be further allowable over Strahm.

CONCLUSION

Based on the foregoing, Appellants request that the Board overturn the rejection of all pending claims and hold that all of the claims of the present application are allowable.

Appellants respectfully petition for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17 for such an extension.

Per MPEP 1204.01, any previously paid appeal fees set forth in 37 CFR 41.20 for filing a Notice of Appeal will be applied to the new Appeal Brief in the same application as long as a final Board decision has not been made on the prior appear. In accordance with MPEP, 1204.01, The Director is hereby authorized to charge any fees which may require, or credit any overpayment to Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: May 5, 2008

Brent E. Vecchia
Agent for Appellants
Registration Number: 48,011

1279 Oakmead Parkway
Sunnyvale, CA 94085
(303)-740-1980

VIII. CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal are:

Claims 1-17 (Cancelled)

18. (Previously Presented) A system comprising:

a network interface couplable with a public network to receive a first client message and first data that is encrypted according to a wireless security format and to receive a second client message and second data that is encrypted according to a wired security format;

a selection system coupled with the network interface to select a first security format conversion for the first data and to select a second security format conversion for the second data; and

a conversion system coupled with the selection system to perform the first security format conversion on the first wireless security format encrypted data and to perform the second security format conversion on the second wired security format encrypted data.

19. (Previously Presented) The system of claim 18, wherein the network interface comprises a first port to receive the first client message and the first data and a second port to receive the second client message and the second data.

20. (Previously Presented) The system of claim 19, wherein the first port has a number selected from the group consisting of the numbers 9208 through 9282, and wherein the second port has number 443.

21. (Previously Presented) The system of claim 20, wherein the first port has the number 9208.

22. (Previously Presented) The system of claim 18, wherein the first data comprises Wireless Transport Layer Security encrypted data, and wherein the second data comprises Secure Sockets Layer encrypted data.

23. (Previously Presented) The system of claim 18, wherein the conversion system comprises a first security format conversion from the wireless security format encrypted data to plain data and a second security format conversion from the wired security format encrypted data to plain data.

24. (Previously Presented) The system of claim 18, wherein the selection system comprises:

logic to receive an indication of one of a plurality of ports of the network interface on which a client message was received from the public network; and

logic to select a security format conversion from among a plurality of format conversions including a first security format conversion from a Wireless Transport Layer Security format to another format and a second security format conversion from a Secure Sockets Layer format to another format in dependence upon the received indication of the port.

25. (Previously Presented) The system of claim 24, wherein the selection system further comprises:

logic to receive information about a security feature supported by a client access device, and wherein the logic to select the security format conversion is capable of selecting one of the plurality of format conversions in dependence upon the received indication of the port and the received information about the security feature supported by the client access device.

26. (Previously Presented) The system of claim 18, wherein the network interface, the selection system, and the conversion system are contained within a single network device.

27. (Previously Presented) The system of claim 26, residing in a data center between the Internet and a data center server.

28. (Previously Presented) The system of claim 26, residing in a data center between a first switch within the data center and a second switch within the data center.

29. (Previously Presented) A method comprising:

listening on a network interface for a first client message and first data that is encrypted according to a security format for wireless data and listening on the network interface for a second client message and second data that is encrypted according to a security format for wired data;

receiving the first client message and the second client message from the network interface;

selecting a first security format conversion for the first data and selecting a second security format conversion for the second data; and

performing the first security format conversion on the first data and performing the second security format conversion on the second data.

30. (Previously Presented) The method of claim 29, wherein said listening on the network interface comprises listening on a first port having a number selected from the group consisting of the numbers 9208 through 9282 for the first client message, and listening on the second port having the number 443 for the second client message.

31. (Previously Presented) The method of claim 29, wherein said selecting comprises selecting a security format conversion from Wireless Transport Layer Security format to another format for the first data and selecting a security format conversion from Secure Sockets Layer format to another format for the second data.

32. (Previously Presented) The method of claim 31, wherein the other formats comprise plain data.

33. (Previously Presented) The method of claim 29:

wherein said listening, receiving, selecting, and performing, are each performed within a single network device; and

wherein the single network device resides within a data center disposed between the Internet and a data center server.

34. (Previously Presented) The method of claim 29:

wherein said listening, receiving, selecting, and performing, are each performed within a single network device; and

wherein the single network device resides within a data center and is disposed between a first data center switch and a second data center switch.

35. (Previously Presented) The method of claim 29, wherein at least a portion of said selecting or said performing is executed in hardware.

36. (Previously Presented) A machine-readable medium having stored thereon data representing sequences of instructions that if executed cause a machine to perform operations comprising:

listening on a network interface for a first client message and first data that is encrypted according to a security format for wireless data and listening on the network interface for a second client message and second data that is encrypted according to a security format for wired data;

receiving the first client message and the second client message from the network interface; and

selecting a first security format conversion for the first data and selecting a second security format conversion for the second data.

37. (Previously Presented) The machine-readable medium of claim 36, wherein the instructions that if executed cause the machine to listen further comprise instructions that if executed cause the machine to listen on a first port having a number selected from the group consisting of the numbers 9208 through 9282 for the first client message, and listening on the second port having the number 443 for the second client message.

38. (Previously Presented) The machine-readable medium of claim 36, wherein the instructions that if executed cause the machine to select further comprise instructions that if executed cause the machine to select a security format conversion from Wireless Transport Layer Security format to another format for the first data and select a security format conversion from Secure Sockets Layer format to another format for the second data.

39. (Previously Presented) The machine-readable medium of claim 38, wherein the other formats comprise plain data.

40. (Previously Presented) A method comprising:

receiving an indication of one of a plurality of ports on which a client message was received from a public network; and

selecting a security format conversion from among a plurality of format conversions including a first security format conversion from a Wireless Transport Layer Security format to another format and a second security format conversion from a Secure Sockets Layer security format to another format in dependence upon the received indication of the port.

41. (Previously Presented) The method of claim 40, wherein the plurality of ports comprise a first port having a number selected from the group consisting of the numbers 9208 through 9282 and a second port having number 443.

42. (Previously Presented) The method of claim 40, wherein the other formats comprise plain data formats.

43. (Previously Presented) The system of claim 23, further comprising a second network interface to provide the plain data.

44. (Previously Presented) The method of claim 32, further comprising providing the plain data from a second network interface.

45. (Previously Presented) The machine-readable medium of claim 39, wherein the instructions further comprise instructions that if executed cause the machine to provide the plain data from a second network interface.

46. (Previously Presented) The method of claim 40, further comprising:

performing the selected security format conversion to plain data; and

providing the plain data to a network through a network interface.

47. (Previously Presented) A system comprising:

a first network interface within a data center and couplable with a public network to receive a first Wireless Transport Layer Security encrypted data from a cell phone client and to receive a second Secure Sockets Layer encrypted data from a personal computer client;

a conversion system within the data center to convert the first Wireless Transport Layer Security encrypted data received from the cell phone client to plain data and to convert the second Secure Sockets Layer encrypted data received from the personal computer client to plain data;

a second network interface within the data center and couplable with a private network to provide the plain data to the private network.

48. (Previously Presented) The system of claim 47, wherein the first and second network interfaces are logically disposed between first and second switches in the data center.

IX. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

To the best of Appellant's knowledge, there is no evidence that is relied upon by Appellants in this appeal to be included in this section.

X. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

(To the best of Appellant's knowledge, there are no related appeals or interferences.)